32

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-143128
(43)Date of publication of application : 16.05.2003

(51)Int.Cl. H04L 9/08
H04L 9/32

(21)Application number : 2001-339959
(22)Date of filing : 05.11.2001

(71)Applicant : OPEN LOOP:KK
(72)Inventor : MURAKAMI SHUICHI

(54) COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To perform high-security communication by simple configuration.
SOLUTION: The ID and PWD of a client terminal are shared off-line (S11 and S12). The client terminal 11 generates a random number value R, calculates Kreg:=h(PWD) to obtain eKreg(R) by ciphers R with Kreg, and transmits ID, h(ID|PWD) and eKreg(R) to an access point 21 (S13 and S14). The access point 21 obtains PWD corresponding to the received ID (S15), obtains h(ID|PWD) (S16), calculates Kreg when matched with a received value (S17), deciphers eKreg(R) by Kreg to extract R (S18), and transmits the hash value of R to the client terminal 11 (S19). When the hash value of R is matched with the received value, the client terminal 11 informs the access point 21 that authentication is OK. After this, KCL:=h(PWD|R) is set to be a ciphering key.

LEGAL STATUS
[Date of request for examination] 12.10.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] Between the 1st equipment (11) and the 2nd equipment (21) which communicate mutually Said the 1st and 2nd equipment share said the 1st Identifier ID and confidential information PWD of equipment, and it sets to said 1st equipment. Generate the predetermined value R and it asks for one-way function value Kreg:=h (PWD) of confidential information PWD. The code data eKreg (R) are calculated by enciphering the predetermined value R, using the one-way function value Kreg of the confidential information for which it asked as a cryptographic key for authentication. To said 2nd equipment Identifier ID The predetermined value eKreg (R) enciphered as the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is transmitted. Said 2nd equipment Search the confidential information PWD corresponding to the identifier ID which received, and the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is calculated. When in agreement as compared with this and the received one-way function value h (ID|PWD), calculate cryptographic key Kreg:=h (PWD) for authentication, and the predetermined value eKreg (R) enciphered using the cryptographic key Kreg for this authentication is decoded. The predetermined value R is extracted and value h (R) which changed this with the tropism function on the other hand is transmitted to said 1st equipment. Said 1st equipment On the other hand, tropism function value h (R) is compared. the predetermined value R of the predetermined value R which asked for tropism function value h (R) on the other hand, and was received with this -- When in agreement, it notifies that authentication was materialized to said 2nd equipment. Said 1st equipment It asks for one-way function value KCL:=h (PWD|R) of connection of confidential information PWD and the predetermined value R as a common key KCL for codes. Said 2nd equipment Common Key KCL: It is the correspondence procedure which calculates =h (PWD|R) and is characterized by what said the 1st equipment and said 2nd equipment communicate mutually, using the common key KCL as a cryptographic key.

[Claim 2] Said 2nd equipment matches and stores said the 1st address and common key KCL of equipment, and distinguishes the address of said 1st equipment at the time of the communication link with said 1st equipment. Read the common key KCL corresponding to the distinguished address, and the read common key KCL is used. The received data from said 1st equipment are decrypted, and the transmit data to said 1st equipment is enciphered. Said 1st equipment The correspondence procedure according to claim 1 which reads the common key KCL of self at the time of the communication link with said 2nd equipment, and is characterized by what the received data from said 2nd equipment are decrypted, and the transmit data to said 2nd equipment is enciphered for using the read common key KCL.
[Claim 3] Said 1st equipment calculates one-way function value Ksave:=h (PIN) of a user's identification information PIN, and makes it the cryptographic key Ksave for preservation, and the common key KCL is enciphered by this cryptographic key Ksave for preservation. It is the correspondence procedure according to claim 1 or 2 which saves the enciphered common key eKsave (KCL) and is characterized by what said 2nd equipment matches and stores said the 1st address and common key of equipment, and Identifier ID and confidential information PWD are canceled for.
[Claim 4] The correspondence procedure according to claim 1, 2, or 3 which generates said the 1st Identifier ID and confidential information PWD of equipment, stores in the storage section with the generation time T with said 2nd equipment, and is characterized by registering Identifier ID and confidential information PWD into delivery and said 1st equipment off-line at said 1st equipment from said 2nd equipment.
[Claim 5] When the identifier which received from said 1st equipment is not able to be detected in the storage section, said 2nd equipment Consider as authentication failure, when the difference of current time and the generation time T is beyond the set point, consider as authentication failure, and it sets to said 2nd equipment. When not in agreement with Identifier ID and the thing of connection of confidential information PWD which, on the other hand, calculated the tropism function value h (ID|PWD), and received, it considers as authentication failure. Said 2nd equipment Search the confidential information PWD corresponding to the identifier ID which received, and the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is calculated. As compared with this and the received one-way function value h (ID|PWD), when not in agreement, it considers as authentication failure. Said 1st equipment It is the correspondence procedure according to claim 4 which asks for tropism function value h (R) on the other hand, and is characterized by what tropism function value h (R) is compared on the other hand, and authentication failure is transmitted for to said 2nd equipment when [of the this and the received predetermined value R of the predetermined value R] not in agreement.
[Claim 6] It is the communication system which communicates between the 1st equipment (11) and the 2nd equipment (21). Said the 1st and 2nd equipment share

said the 1st Identifier ID and confidential information PWD of equipment. Said 1st equipment Generate the predetermined value R and one-way function value Kreg:=h (PWD) of confidential information PWD is calculated. The code data eKreg (R) are calculated by enciphering the predetermined value R, using the one-way function value Kreg of the calculated confidential information as a cryptographic key for authentication. To said 2nd equipment Identifier ID The predetermined value eKreg (R) enciphered as the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is transmitted. Said 2nd equipment Search the confidential information PWD corresponding to the identifier ID which received, and the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is calculated. Compare this with the received one-way function value h (ID|PWD), and when in agreement, calculate cryptographic key Kreg:=h (PWD) for authentication, and the predetermined value eKreg (R) enciphered using the cryptographic key Kreg for this authentication is decoded. The predetermined value R is extracted and value h (R) which changed this with the tropism function on the other hand is transmitted to said 1st equipment. Said 1st equipment On the other hand, tropism function value h (R) is compared. the predetermined value R of the predetermined value R which asked for tropism function value h (R) on the other hand, and was received with this -- When in agreement, it notifies that authentication was materialized to said 2nd equipment. Said 1st equipment In quest of one-way function value KCL:=h (PWD|R) of connection of confidential information PWD and the predetermined value R, it saves as a common key KCL for codes. Said 2nd equipment Common Key KCL: It is the communication system which calculates and saves =h (PWD|R) and is characterized by what said the 1st equipment and said 2nd equipment communicate mutually, using the common key KCL as a cryptographic key.

[Claim 7] Between the 1st equipment (11) and the 2nd equipment (21) which communicate mutually The private key KCL of said 1st equipment is generated, and the address of said 1st equipment and the pair of this private key KCL are notified and registered into said 2nd equipment off-line. Said 2nd equipment The self private key KAP is generated at the time of an idle. Said 2nd equipment Receive the connection request from said 1st equipment, and the private key KCL of said 1st equipment is searched from the address of said 1st equipment of a requiring agency. Generate the session key K, and encipher connection to the predetermined value R, and the session key K and the self private key KAP with the private key KCL of said 1st equipment, and the code data eKCL (R|K|KAP) are generated. It transmits to said 1st equipment. Said 1st equipment The self-addressed code data eKCL (R|K|KAP) are decoded with the self private key KCL. The predetermined value R, and the session key K and the private key KAP of said 2nd equipment are extracted. Furthermore, encipher the extracted predetermined value R with the private key KAP of said 2nd equipment, and the code data eKAP (R) are generated. The generated code data

eKAP (R) are transmitted to said 2nd equipment. Said 2nd equipment Receive the code data eKAP (R), decode this with the private key KAP of said 2nd equipment, compare the predetermined value R which extracted and extracted the predetermined value R with the predetermined value R transmitted to said 1st equipment, and if in agreement It distinguishes from authentication formation. Said the 1st equipment and said 2nd equipment Respectively, it is the correspondence procedure which saves the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment, and is henceforth characterized by what said the 1st equipment and said 2nd equipment perform cryptocommunication for using the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment.

[Claim 8] When said the 1st address and common key KCL of equipment are matched and stored and it communicates between said 2nd equipment and said each 1st equipment, said 2nd equipment said 2nd equipment Distinguish the address of said 1st equipment and the common key KCL corresponding to the distinguished address is read. Using the read common key KCL, the received data from said 1st equipment are decrypted, and the transmit data to said 1st equipment is enciphered. Said 1st equipment At the time of the communication link with said 2nd equipment, read the common key KCL of self and the read common key KCL is used. Decrypt the received data from said 2nd equipment, and the transmit data to said 2nd equipment is enciphered. When transmitting data common to said two or more 1st equipments from said 2nd equipment, said 2nd equipment The self private key KAP is read and the transmit data to said two or more 1st equipments is enciphered using the read private key KAP. Said 1st equipment The correspondence procedure according to claim 7 which reads the private key KAP of said 2nd equipment, and is characterized by what the received data from said 2nd equipment are decrypted for using the read private key KAP.

[Claim 9] Said 2nd equipment enciphers and sends out data with the private key KAP of said 2nd equipment, when the transmission place address of the data for transmission is a broadcast address. Each 1st equipment of the above The received data are decrypted with the private key KAP of said 2nd equipment. A destination address When the storage section memorizes, the data for transmission are enciphered and sent out with the private key KCL corresponding to the address of a transmission place. Said 1st equipment The correspondence procedure according to claim 7 or 8 characterized by what the data for transmission are canceled for when self-addressed data are decrypted with the self private key KCL and the destination address is not memorized by the storage section.

[Claim 10] It is the communication system which communicates between the 1st equipment (11) and the 2nd equipment (21). The private key KCL of said 1st equipment is generated. The address of said 1st equipment, and the pair of this private key KCL It notifies to said 2nd equipment off-line, and this is registered into the storage section. Said 2nd equipment The self private key KAP is generated and

stored at the time of an idle. Said 2nd equipment Receive the connection request from said 1st equipment, and the private key KCL of said 1st equipment is searched from the address of said 1st equipment of a requiring agency. Generate the session key K, and encipher connection to the predetermined value R, and the session key K and the self private key KAP with the private key KCL of said 1st equipment, and the code data eKCL (R|K|KAP) are generated. It transmits to said 1st equipment. Said 1st equipment The self-addressed code data eKCL (R|K|KAP) are decoded with the self private key KCL. The predetermined value R, and the session key K and the private key KAP of said 2nd equipment are extracted. Furthermore, encipher the extracted predetermined value R with the private key KAP of said 2nd equipment, and the code data eKAP (R) are generated. The generated code data eKAP (R) are transmitted to said 2nd equipment. Said 2nd equipment If receive the code data eKAP (R), this is decoded with a private key KAP, the predetermined value R is extracted and it is in agreement as compared with the extracted predetermined value R and the sent predetermined value R which was transmitted to said 1st equipment It distinguishes from authentication formation. Said the 1st equipment and said 2nd equipment Respectively, it is the communication system which saves the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment, and is henceforth characterized by what said the 1st equipment and said 2nd equipment perform cryptocommunication for using the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment.

[Claim 11] The computer program for operating a computer as claim 5, the 1st equipment of 10, or the 2nd equipment.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a cryptocommunication system and an approach.

[0002]

[Description of the Prior Art] The wireless LAN of IEEE802.11b conformity has spread as a cheap and easy wireless LAN construction device.

[0003]

[Problem(s) to be Solved by the Invention] However, the problem on "security" is pointed out to IEEE802.11b. That is, the security protocol WEP (Wired Equivalency Privacy) of IEEE802.11b is brittle, and has risk of communicative security not being maintained. The same problem corresponds also to a communication link with a cable,

and the simpler cryptocommunication system of high reliance, a cryptocommunication protocol, etc. are desired.
[0004] This invention was made in view of the situation mentioned above, and aims at offering the system and approach of performing a reliable communication link. moreover, a configuration with this easy invention -- it is -- high -- it sets it as other purposes to enable a security communication link.
[0005]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the correspondence procedure concerning the 1st viewpoint of this invention Between the 1st equipment (11) and the 2nd equipment (21) which communicate mutually Said the 1st and 2nd equipment share said the 1st Identifier ID and confidential information PWD of equipment, and it sets to said 1st equipment. Generate the predetermined value R and it asks for one-way function value Kreg:=h (PWD) of confidential information PWD. The code data eKreg (R) are calculated by enciphering the predetermined value R, using the one-way function value Kreg of the confidential information for which it asked as a cryptographic key for authentication. To said 2nd equipment Identifier ID The predetermined value eKreg (R) enciphered as the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is transmitted. Said 2nd equipment Search the confidential information PWD corresponding to the identifier ID which received, and the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is calculated. When in agreement as compared with this and the received one-way function value h (ID|PWD), calculate cryptographic key Kreg:=h (PWD) for authentication, and the predetermined value eKreg (R) enciphered using the cryptographic key Kreg for this authentication is decoded. The predetermined value R is extracted and value h (R) which changed this with the tropism function on the other hand is transmitted to said 1st equipment. Said 1st equipment On the other hand, tropism function value h (R) is compared. the predetermined value R of the predetermined value R which asked for tropism function value h (R) on the other hand, and was received with this -- When in agreement, it notifies that authentication was materialized to said 2nd equipment. Said 1st equipment It asks for one-way function value KCL:=h (PWD|R) of connection of confidential information PWD and the predetermined value R as a common key KCL for codes. Said 2nd equipment Common Key KCL: =h (PWD|R) is calculated and said the 1st equipment and said 2nd equipment are characterized by what is communicated mutually, using the common key KCL as a cryptographic key.
[0006] For example, said 2nd equipment matches and stores said the 1st address and common key KCL of equipment, and distinguishes the address of said 1st equipment at the time of the communication link with said 1st equipment. Read the common key KCL corresponding to the distinguished address, and the read common key KCL is used. The received data from said 1st equipment are decrypted, and the transmit data to said 1st equipment is enciphered. Said 1st equipment At the time of the

communication link with said 2nd equipment, the common key KCL of self is read, using the read common key KCL, the received data from said 2nd equipment are decrypted, and the transmit data to said 2nd equipment is enciphered.
[0007] Said 1st equipment calculates one-way function value Ksave:=h (PIN) of a user's identification information PIN, and makes it the cryptographic key Ksave for preservation, and the common key KCL is enciphered by this cryptographic key Ksave for preservation. the enciphered common key eKsave (KCL) is saved, said 2nd equipment matches and stores said the 1st address and common key of equipment, and Identifier ID and confidential information PWD are canceled -- it is good even if like.
[0008] With said 2nd equipment, said the 1st Identifier ID and confidential information PWD of equipment are generated, it stores in the storage section with the generation time T, and you may make it register Identifier ID and confidential information PWD into said 1st equipment off-line from said 2nd equipment at delivery and said 1st equipment.
[0009] in this case, when the identifier which received from said 1st equipment is not able to be detected in the storage section, said 2nd equipment Consider as authentication failure, when the difference of current time and the generation time T is beyond the set point, consider as authentication failure, and it sets to said 2nd equipment. When not in agreement with Identifier ID and the thing of connection of confidential information PWD which, on the other hand, calculated the tropism function value h (ID|PWD), and received, it considers as authentication failure. Said 2nd equipment the case where search the confidential information PWD corresponding to the identifier ID which received, calculate the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD), and it is not in agreement with this as compared with the received one-way function value h (ID|PWD) -- authentication -- it is good also as abortive. Moreover, on the other hand, tropism function value h (R) is compared, and when [of the this and the received predetermined value R of the predetermined value R] not in agreement, you may make it said 1st equipment transmit authentication failure to said 2nd equipment by on the other hand asking for tropism function value h (R).
[0010] In order to attain the above-mentioned purpose, the communication system concerning the 2nd viewpoint of this invention It is the communication system which communicates between the 1st equipment (11) and the 2nd equipment (21). Said the 1st and 2nd equipment share said the 1st Identifier ID and confidential information PWD of equipment. Said 1st equipment Generate the predetermined value R and one-way function value Kreg:=h (PWD) of confidential information PWD is calculated. The code data eKreg (R) are calculated by enciphering the predetermined value R, using the one-way function value Kreg of the calculated confidential information as a cryptographic key for authentication. To said 2nd equipment Identifier ID The predetermined value eKreg (R) enciphered as the one-way function value h of

connection to Identifier ID and confidential information PWD (ID|PWD) is transmitted. Said 2nd equipment Search the confidential information PWD corresponding to the identifier ID which received, and the one-way function value h of connection to Identifier ID and confidential information PWD (ID|PWD) is calculated. Compare this with the received one-way function value h (ID|PWD), and when in agreement, calculate cryptographic key Kreg:=h (PWD) for authentication, and the predetermined value eKreg (R) enciphered using the cryptographic key Kreg for this authentication is decoded. The predetermined value R is extracted and value h (R) which changed this with the tropism function on the other hand is transmitted to said 1st equipment. Said 1st equipment On the other hand, tropism function value h (R) is compared. the predetermined value R of the predetermined value R which asked for tropism function value h (R) on the other hand, and was received with this -- When in agreement, it notifies that authentication was materialized to said 2nd equipment. Said 1st equipment It asks for one-way function value KCL:=h (PWD|R) of connection of confidential information PWD and the predetermined value R as a common key KCL for codes. Said 2nd equipment Common Key KCL: =h (PWD|R) is calculated and said the 1st equipment and said 2nd equipment are characterized by what is communicated mutually, using the common key KCL as a cryptographic key.

[0011] In order to attain the above-mentioned purpose, the correspondence procedure concerning the 3rd viewpoint of this invention Between the 1st equipment (11) and the 2nd equipment (21) which communicate mutually The private key KCL of said 1st equipment is generated, and the address of said 1st equipment and the pair of this private key KCL are notified and registered into said 2nd equipment off-line. Said 2nd equipment The self private key KAP is generated at the time of an idle. Said 2nd equipment Receive the connection request from said 1st equipment, and the private key KCL of said 1st equipment is searched from the address of said 1st equipment of a requiring agency. Generate the session key K, and encipher connection to the predetermined value R, and the session key K and the self private key KAP with the private key KCL of said 1st equipment, and the code data eKCL (R|K|KAP) are generated. It transmits to said 1st equipment. Said 1st equipment The self-addressed code data eKCL (R|K|KAP) are decoded with the self private key KCL. The predetermined value R, and the session key K and the private key KAP of said 2nd equipment are extracted. Furthermore, encipher the extracted predetermined value R with the private key KAP of said 2nd equipment, and the code data eKAP (R) are generated. The generated code data eKAP (R) are transmitted to said 2nd equipment. Said 2nd equipment Receive the code data eKAP (R), decode this with the private key KAP of said 2nd equipment, compare the predetermined value R which extracted and extracted the predetermined value R with the predetermined value R transmitted to said 1st equipment, and if in agreement It distinguishes from authentication formation. Said the 1st equipment and said 2nd equipment Respectively, the private key KCL of said 1st equipment and the private key KAP of

said 2nd equipment are saved, and said the 1st equipment and said 2nd equipment are henceforth characterized by what cryptocommunication is performed for using the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment.

[0012] For example, when said 2nd equipment matches and stores said the 1st address and common key KCL of equipment and it communicates between said 2nd equipment and said each 1st equipment, said 2nd equipment distinguishes the address of said 1st equipment. Read the common key KCL corresponding to the distinguished address, and the read common key KCL is used. The received data from said 1st equipment are decrypted, and the transmit data to said 1st equipment is enciphered. Said 1st equipment At the time of the communication link with said 2nd equipment, read the common key KCL of self and the read common key KCL is used. Decrypt the received data from said 2nd equipment, and the transmit data to said 2nd equipment is enciphered. When transmitting data common to said two or more 1st equipments from said 2nd equipment, said 2nd equipment The self private key KAP is read and the transmit data to said two or more 1st equipments is enciphered using the read private key KAP. Said 1st equipment The private key KAP of said 2nd equipment is read, and the received data from said 2nd equipment are decrypted using the read private key KAP.

[0013] For example, when the transmission place address of the data for transmission of said 2nd equipment is a broadcast address, Data are enciphered and sent out with the private key KAP of said 2nd equipment. Each 1st equipment of the above The received data are decrypted with the private key KAP of said 2nd equipment. A destination address When the storage section memorizes, the data for transmission are enciphered and sent out with the private key KCL corresponding to the address of a transmission place. Said 1st equipment When self-addressed data are decrypted with the self private key KCL and the destination address is not memorized by the storage section, the data for transmission are canceled.

[0014] In order to attain the above-mentioned purpose, the communication system concerning the 4th viewpoint of this invention It is the communication system which communicates between the 1st equipment (11) and the 2nd equipment (21). The private key KCL of said 1st equipment is generated. The address of said 1st equipment, and the pair of this private key KCL It notifies to said 2nd equipment off-line, and this is registered into the storage section. Said 2nd equipment The self private key KAP is generated and stored at the time of an idle. Said 2nd equipment Receive the connection request from said 1st equipment, and the private key KCL of said 1st equipment is searched from the address of said 1st equipment of a requiring agency. Generate the session key K, and encipher connection to the predetermined value R, and the session key K and the self private key KAP with the private key KCL of said 1st equipment, and the code data eKCL (R|K|KAP) are generated. It transmits to said 1st equipment. Said 1st equipment The self-addressed code data eKCL

(R|K|KAP) are decoded with the self private key KCL. The predetermined value R, and the session key K and the private key KAP of said 2nd equipment are extracted. Furthermore, encipher the extracted predetermined value R with the private key KAP of said 2nd equipment, and the code data eKAP (R) are generated. The generated code data eKAP (R) are transmitted to said 2nd equipment. Said 2nd equipment If receive the code data eKAP (R), this is decoded with a private key KAP, the predetermined value R is extracted and it is in agreement as compared with the extracted predetermined value R and the sent predetermined value R which was transmitted to said 1st equipment It distinguishes from authentication formation. Said the 1st equipment and said 2nd equipment Respectively, the private key KCL of said 1st equipment and the private key KAP of said 2nd equipment are saved, and said the 1st equipment and said 2nd equipment are henceforth characterized by what cryptocommunication is performed for using the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment.

[0015] Creation, distribution, etc. may carry out the program for operating a computer as the 1st equipment of the above, or the 2nd equipment, or making a computer perform actuation of the 1st equipment of the above, or the 2nd equipment.

[0016]

[Embodiment of the Invention] Hereafter, the communication system and the correspondence procedure concerning the gestalt of operation of this invention are explained with reference to a drawing.

[0017] The communication system concerning the gestalt of this operation consists of Gateway servers 31 which were connected to the access point (server) 21 which constitutes wireless LAN 41, and the access point 21 through the cable LAN 42 etc. between two or more client terminals (user terminal) 11 (111-11n) and the client terminal 11, and were connected to the external network, as shown in drawing 1 .

[0018] As each client terminal 11 consists of a personal computer, a workstation, etc. and is shown in drawing 2 , it has the storage section 111, the input section 112, and a display 113 and the processing section 114, and is equipped with the wireless LAN card 12.

[0019] The storage section 111 consists of RAM, a ROM, a hard disk, etc., and memorizes various data and programs. In the gestalt of this operation, programs of operation, such as data, such as the identifier ID in the end of a local, Password PWD, the random-number value R, a private key KCL, the key Kreg for registration, and the key Ksave for preservation, an authentication program, an encryption program, an application program, and a communications program, are memorized.

[0020] The input section 112 is equipped with a keyboard, a mouse, a record-medium I/O device, etc., and supplies various data and directions to the processing section 114. A display 113 displays various information.

[0021] The processing section 114 is equipped with a processor etc. and operates according to the program of operation memorized by the storage section 111.

Authentication processing and cryptocommunication processing are performed in the example of a gestalt of this operation. Moreover, the processing section 114 is equipped with the timer.

[0022] The wireless LAN card 12 receives and decodes the radio signal which is constituted as the so-called PC card and the client terminal 11 is equipped with, and changes into a radio signal the transmit data supplied from the processing section 114, and transmits to an access point 21, and an access point 21 transmits, and provides the processing section 114 with it. In the wireless LAN card 12, the MAC (Machine Access Control) address of the proper for identifying the card is memorized.

[0023] an access point 21 -- between two or more client terminals 11 -- wireless LAN 41 -- constituting -- wireless LAN 41 and a cable LAN 42 -- ** -- it is for data to transmit in between, and as shown in drawing 3 , it has wireless (interface) IF 211, a cable (interface) IF 212, the storage section 213, a database 214, the input section 215, a display 216, and the processing section 217.

[0024] Wireless IF 211 changes into a radio signal the transmit data which receives the radio signal from the client terminal 11, gets over, and provides for the processing section 217, and is offered from the processing section 217, and carries out wireless transmission.

[0025] A cable IF 212 sends out the signal which provides the processing section 217 with the signal on a cable LAN 42, and is offered from the processing section 217 on a cable LAN 42.

[0026] The storage section 213 consists of RAM, a ROM, a hard disk, etc., and memorizes various data and programs. In the gestalt of this operation, programs of operation, such as data, such as the random-number value R, a private key KCL, the key Kreg for registration, and the key Ksave for preservation, an authentication program, an encryption program, an application program, and a communications program, are memorized.

[0027] A database (DB) 214 contains the registration information DB and the client key DB, as shown in drawing 4 . The registration information DB matches and memorizes the generation time T of the identifier ID of each client terminal 11, Password (presetting confidential information) PWD, and Identifier ID and Password PWD. The client key DB matches and memorizes the MAC Address and the client key (secret cryptographic key; common key) KCL of the wireless LAN card 12 with which the client terminal 11 was equipped.

[0028] The input section 215 of drawing 3 is equipped with a keyboard, a mouse, a record-medium I/O device, etc., and supplies various data and directions to the processing section 217. A display 216 displays various information.

[0029] The processing section 217 is equipped with a processor etc. and operates according to the program of operation memorized by the storage section. Especially, in the gestalt of this operation, wireless cryptocommunication processing including authentication processing of the client terminal 11 etc. and bridge processing of the

data between wireless LAN 41 and a cable LAN 42 are performed. About the detail of processing, it mentions later.
[0030] It connects with a cable LAN 42 and the Gateway server 31 of drawing 1 is connected to the network of the exteriors, such as INTANETTOIN IN.
[0031] Next, actuation of the communication system which has the above-mentioned configuration is explained. In this communication system, in order to receive data through the wireless LAN 41 built between the client terminal 11 and an access point 21, as shown in drawing 5 , it is necessary to complete prior registration and the procedure of mutual recognition.
[0032] (1) When newly connecting the client terminal 11 to the prior registration wireless LAN 41 to the access point 21 of the client terminal 11, the manager of a system is an access point 21, he generates ID and Password PWD in advance (step S11), and as shown in the registration information DB with the generation time T at drawing 4 (a), he registers.
[0033] Identifier ID and Password PWD which were generated are notified to the client terminal 11 off-line, for example, are entered from the input section 213, and are registered into the storage section 111 (step S12). Thereby, new Identifier ID and new Password PWD of the client terminal 11 are shared between the client terminal 11 and an access point 21.
[0034] (2) The client terminal 11, the mutual recognition of an access point 21, and exchange a of a cryptographic key The client terminal 11 requires connection of an access point 21 to communicate through wireless LAN 41. Answering this demand, an access point 21 once establishes connection by radio between the client terminals 11 according to opening authentication.
[0035] b) Next, the processing section 114 of the client terminal 11 performs a random-number program, and generates the random-number value R (the constant of arbitration is sufficient although a random number is desirable in addition). Furthermore, by predetermined Hash Function h ( ), the processing section 114 calculates the password PWD defined by several 1, the hash value of connection to the random-number value R, and the hash value of Password PWD, considers as the client key KCL of the client terminal 11, and the key Kreg for registration, and is stored in the storage section 111 (step S13). In addition, the client key KCL is a private key common to a client 11 and an access point 21, and the key Kreg for registration is a common key used only for authentication processing.
[Equation 1] KCL:=h(PWD|R)
Kreg:=h(PWD)
It is the communication system which communicates between the 1st equipment (11) and the 2nd equipment (21). The private key KCL of said 1st equipment is generated. The address of said 1st equipment, and the pair of this private key KCL It notifies to said 2nd equipment off-line, and this is registered into the storage section. Said 2nd equipment The self private key KAP is generated and stored at the time of an idle.

Said 2nd equipment Receive the connection request from said 1st equipment, and the private key KCL of said 1st equipment is searched from the address of said 1st equipment of a requiring agency. Generate the session key K, and encipher connection to the predetermined value R, and the session key K and the self private key KAP with the private key KCL of said 1st equipment, and the code data eKCL (R|K|KAP) are generated. It transmits to said 1st equipment. Said 1st equipment The self-addressed code data eKCL (R|K|KAP) are decoded with the self private key KCL. The predetermined value R, and the session key K and the private key KAP of said 2nd equipment are extracted. Furthermore, encipher the extracted predetermined value R with the private key KAP of said 2nd equipment, and the code data eKAP (R) are generated. The generated code data eKAP (R) are transmitted to said 2nd equipment. Said 2nd equipment If receive the code data eKAP (R), this is decoded with a private key KAP, the predetermined value R is extracted and it is in agreement as compared with the extracted predetermined value R and the sent random-number value R which was transmitted to said 1st equipment It distinguishes from authentication formation. Said the 1st equipment and said 2nd equipment It is [0036] to which the private key KCL of said 1st equipment and the private key KAP of said 2nd equipment are saved 0036, and said the 1st equipment and said 2nd equipment perform cryptocommunication henceforth using the private key KCL of said 1st equipment, and the private key KAP of said 2nd equipment, respectively. c) Next, generate the encryption data eKreg (R) based on hash value h (ID|PWD) of connection in Identifier ID and Password PWD, and the key Kreg for registration of the random-number value R, and store in the storage section 111 temporarily. In addition, hash value h (ID|PWD) of connection in Identifier ID and Password PWD should just be calculated by even the transmitting phase at either the access point 21 or the client terminal 11.

[0037] d) Then, the client terminal 11 transmits the self identifier ID, hash value h (ID|PWD), and the code data eKreg (R) to an access point 21 (step S14).

[0038] e) The processing section 217 of an access point 21 receives these data through wireless IF 211, and once stores them in the storage section 213. Then, the registration information DB is retrieved for the identifier ID which received to a key.

[0039] f) this retrieval processing -- when it is and the identifier ID which received is not registered into the registration information DB, judge that it is unlawful access, return an unlawful access error, and cut connection with that client terminal 11 henceforth (step S15). On the other hand, when the identifier ID is registered into the registration information DB, the corresponding password PWD and the generation time T are read.

[0040] g) Next, search for the difference of the generation time T and current time which were read, and distinguish whether it is beyond a reference value.

g-1) When **** of the generation time T and current time is over the reference value (i.e., when a long period of time has passed since registration), answer the client

terminal 11 through wireless IF 211 in a registration time-out. The processing section 114 of the client terminal 11 displays the message of a purport which should receive through the wireless LAN card 12 and should re-register this into a display 113.
[0041] g-2) On the other hand, when the difference of the generation time T and the time of present in Japan is under a reference value (i.e., when not equivalent to a registration time-out), the processing section 217 verifies hash value h (ID|PWD) (step S16). That is, it distinguishes whether the processing section 217 is in agreement with hash value h (ID|PWD) which calculated hash value h (ID|PWD) of connection in the identifier ID which received, and the password PWD read from the registration information DB, and received from the client terminal 11. When in agreement and it distinguishes, the processing section 217 returns challenge failure to the client terminal 11, and cuts connection.
[0042] h) When calculated hash value h (ID|PWD) and hash value h (ID|PWD) which received were in agreement and it distinguishes on the other hand, the processing section 217 calculates the key Kreg for registration (: =h (PWD)) (step S17).
[0043] Next, the processing section 217 decodes the encryption data eKreg of the received random-number value R (R) using the generated key Kreg for registration, and extracts the random-number value R which the client terminal 11 generated previously (step S18).
[0044] i) The processing section 217 calculates hash value [of the extracted random-number value R] h (R), and transmits this to the client terminal 11 (step S19).
[0045] j) Next, the processing section 114 of the client terminal 11 verifies hash value [of the random-number value R] h (R) (step S20). That is, the processing section 114 calculates hash value [of the random-number value R memorized in the storage section 111] h (R), and compares with this hash value h (R) which received from the access point 21. When both hash values are not in agreement, they return "authentication failure (NG)" to an access point 21, and the processing section 114 cuts connection. On the other hand, when it is judged that it is in agreement, "an authentication success (O.K.)" is returned to an access point 21.
[0046] k) Answering the notice of an authentication success, the processing section 217 of an access point 21 calculates client key KCL:=h (PWD|R) (step S21), and registers {a MAC Address and KCL} into the client key DB of a database 214 using the MAC Address contained in the header information of radio. Then, Identifier ID and Password PWD on the storage section 213 are canceled.
[0047] l) The processing section 114 of the client terminal 11 inputs PIN (identification information) of the user by whom the user is recorded on the IC card for authentication etc. from the input section 112, for example, after transmitting an authentication success. The processing section 114 calculates hash value:=h (PIN) of inputted PIN, and is taken as the key Ksave for preservation. Using this key Ksave for preservation, the processing section 114 enciphers the client key KCL, and saves the enciphered client key eKsave (KCL) in the storage section 111.

[0048] In the above comparatively easy procedure, the mutual recognition between the client terminal 11 and an access point 21 and exchange of a cryptographic key are completed safely, and a wireless code channel is established.
[0049] For example, in transmitting the packet received through Cable LAN side to the cable IF 212 to the client terminal 11 from an access point 21 at a wireless LAN side, it performs the next processing.
[0050] First, the MAC Address of the destination of the packet which received is distinguished and it distinguishes whether this MAC Address is registered into the client key database. When were registered, it distinguishes and the MAC Address exists in a table, the client key KCL corresponding to the MAC Address is read, the part (payload) except the packet header of a packet is enciphered with the client key KCL, and it sends out from wireless IF 211.
[0051] The processing section 114 of each client terminal 11 incorporates radio intelligence through a radio communication equipment 12. The processing section 114 asks for hash value h (PIN) of a user's PIN, asks for the key Ksave for preservation, and decodes the enciphered client key eKsave (KCL) which is stored in the storage section 111 using this key Ksave for preservation. Using the decrypted client key KCL, the processing section 114 decrypts the payload part of a self-addressed packet, and memorizes it in the storage section 111.
[0052] On the other hand, a radio communication equipment 12 cancels this, when the MAC Address contained in the header differs from a self MAC Address. By this, a packet will receive only the packet enciphered with the client key KCL of self by self-addressed.
[0053] On the other hand, an access point 21 cancels the packet, when it is judged that the MAC Address of the packet for transmission does not exist in the client key DB.
[0054] In case a packet is sent out from the client terminal 11 to an access point 21, it enciphers with the client key KCL which generated the key Ksave for preservation, decrypted the client key KCL with this key Ksave for preservation, and decrypted the information storing part (payload) of a packet from a user's PIN, and the processing section 114 is sent out from the wireless LAN card 12.
[0055] The processing section 217 of an access point 21 once incorporates a radio signal through wireless IF 211, distinguishes the Mac address of a transmitting agency from header information, reads the client key KCL corresponding to this from the client key DB, and decrypts a payload part. If an access point 21 is required, after it enciphers this by the encryption algorithm for Cables LAN, it sends out a packet to Cable LAN.
[0056] (3) When the client terminal 11 stops existing under management of the communicative cutting access point 21, an access point 21 cuts connection and stands by the connection request from a client.
[0057] As explained above, this communication system can carry out exchange of the

mutual recognition between the client terminal 11 and an access point 21, and a cryptographic key to insurance in a comparatively easy procedure. It is designed based on the common key encryptosystem. For this reason, as compared with the case where a public key system is used, it becomes possible to raise processing speed.

[0058] Moreover, since the private key KCL of each client terminal 11 is registered into an access point 21 and it is used by authentication processing, spoofing can be prevented.

[0059] (Gestalt of the 2nd operation) The gestalt of operation of the 2nd of the communication system concerning the gestalt of implementation of this invention is explained hereafter.

[0060] The basic configuration of the system of the gestalt of this operation is substantially the same, and is hereafter explained to be the structure of a system of the gestalt of the 1st operation focusing on the communications protocol which is the focus.

[0061] (1) The processing section 114 generates the private key KCL of a client on the client terminal 11 with which registration **** of a client and the wireless LAN card 12 were installed.

[0062] Next, the MAC Address of the wireless LAN card 12 and the pair of this common key KCL are transmitted to an access point 21 off-line. An access point 21 registers this pair into a database 214.

[0063] (2) At the time of the idle, the processing section 217 of the generation access point 21 of an access point key generates the private key KAP of an access point 21 dynamically, and stores it in the storage section 213 (when the client terminal 11 which is communicating does not exist).

[0064] (3) The authentication access point 21 of the client terminal 11 performs key exchange and authentication in the following procedure, when the connection request from the client terminal 11 is received.

[0065] a). The client terminal 11 transmits a connection request to an access point 21.

[0066] b). The processing section 217 of an access point 21 receives a connection request, accesses a database 214, and searches the client key KCL from the MAC Address of the client terminal 11.

[0067] c). The processing section 217 of an access point 21 generates the session key K at random.

d). The processing section 217 of an access point 21 enciphers connection in the random-number value R, and the session key K and the access point key KAP with the client key KCL, and generates the code data eKCL (R|K|KAP).

[0068] e). The processing section 217 of an access point 21 transmits the code data eKCL (R|K|KAP) to the client terminal 11 through wireless IF 211.

[0069] f). Through the wireless LAN card 12, the processing section 114 of the client

terminal 11 decodes the self-addressed code data eKCL (R|K|KAP) with the client key KCL of self, and extracts the random-number value R, the session key K, and the access point key KAP.
[0070] g). The processing section 114 of the client terminal 11 enciphers the random-number value R with the access point key KAP, and generates the code data eKAP (R).
[0071] h). The processing section 114 of the client terminal 11 transmits the generated encryption data eKAP (R) to an access point 21.
[0072] i) . The processing section 217 of an access point 21 receives the encryption data eKAP (R) through wireless IF 211, decodes this with the access point key KAP, and extracts the random-number value R.
[0073] j). An access point 21 compares the extracted random-number value R with the random-number value R generated previously, and if in agreement, it will judge it to be "an authentication success (O.K.)."
[0074] Thus, after authentication of the client terminal 11 is successful, wireless cryptocommunication is performed between the client terminal 11 and an access point 21.
[0075] For example, in case an access point 21 transmits the packet received from the cable LAN 42 side to a wireless LAN 41 side, the processing section 217 performs the following processings according to the value of a MAC Address.
[0076] a). First, when the transmission place address of the packet which received through the cable IF 212 is a broadcast address, a control section 217 enciphers the payload of a packet with the access point key KAP, and sends it out to wireless IF 211. Each client terminal 11 receives a packet, distinguishes that a destination address is a broadcast address, and decrypts a payload with the access point key KAP stored in the storage section 111.
[0077] b). A control section 217 distinguishes whether in the case of the MAC Address, the destination address is registered into the database 214 for the transmission place address of the packet which received through the cable IF 212. When registered, the client key KCL corresponding to the MAC Address is read, the payload of the packet is enciphered with the client key KCL, and it sends out to wireless IF 211. Each client terminal 11 distinguishes a self-addressed packet, and decrypts a payload with the client key KCL stored in the storage section 111.
[0078] c). When the destination address is not registered into a database 214, the processing section 217 cancels the packet.
[0079] On the other hand, in transmitting data to an access point 21 from the client terminal 11, the processing section 114 of each client terminal 11 enciphers the payload of a packet with the client key KCL of self, and sends it out to the wireless LAN card 12. An access point 21 distinguishes a transmitting agency from the transmitting agency address, reads the client key KCL corresponding to this from the table on a database 214, and decrypts the payload of a packet with the client key

KCL.
[0080] Since the communication system of the gestalt of this 2nd operation is also designed based on the common key encryptosystem, it can make processing speed high. Moreover, since the private key of a client is registered beforehand and it is used by authentication processing, spoofing can be prevented. Moreover, the key of an access point is generated dynamically, key exchange is performed with the client terminal, and the brittleness by IV collision which is the weak spot of WEP can be avoided.
[0081] In addition, this invention is not limited to the gestalt of the above-mentioned implementation, but various deformation and application are possible for it. For example, although the gestalt of the above 1st and the 2nd operation has illustrated the solution powerful as a basic algorithm, it can also be simplified if needed. On the contrary, other requirements for verification may be added in the case of authentication. In this invention, with "an authentication success", when other requirements or conditions exist, let it be requirements to have satisfied them.
[0082] Other functions may be used although the Hash Function was illustrated as a tropism function on the other hand with the gestalt of the above-mentioned implementation. In the gestalt of the above-mentioned implementation, in the communication link between a client and an access point, although this invention was explained to the example, this invention is not limited to this, but when performing cryptocommunication between two equipments, it can apply widely. Moreover, although this invention was explained to the example, this invention is not limited to wireless LAN, but can apply wireless LAN also to other radio. Furthermore, it is applicable also to a wire communication. In the case of a wire communication, except that the wireless LAN card 12 is changed into a LAN card and wireless IF 211 is changed into Cable IF, there is no ontic modification.
[0083] In addition, the system of this invention cannot be based on the system of dedication, but can be realized using the usual computer system. For example, the server 111 grade which performs above-mentioned processing can be constituted by installing this program from the media (a flexible disk, CD-ROM, etc.) which stored the program for performing above-mentioned actuation in the computer. In addition, an above-mentioned function may be stored only through parts other than OS, when OS is realized by cooperation of an assignment or OS, and application.
[0084] In addition, it is also possible to superimpose a program on a subcarrier and to distribute through a communication network. For example, this program may be put up for the notice plate (BBS) of a communication network, and this may be distributed through a network. And above-mentioned processing can be performed by starting this program and making it perform like other application programs under control of OS.
[0085]
[Effect of the Invention] According to this invention, it becomes possible to perform a

reliable communication link.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the communication system concerning the operation gestalt of this invention.

[Drawing 2] It is drawing showing the configuration of the client terminal shown in drawing 1 .

[Drawing 3] It is drawing showing the configuration of the access point shown in drawing 1 .

[Drawing 4] It is drawing showing the example of the table stored in the database shown in drawing 3 .

[Drawing 5] In the gestalt of the 1st operation, it is drawing showing the information transmitted and received between a client terminal and an access point, and its procedure.

[Description of Notations]

11 Client Terminal

21 Access Point

41 Wireless LAN

42 Cable LAN

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－143128
（P2003－143128A）
(43)公開日　平成15年５月16日(2003.5.16)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ　５Ｊ１０４
9/32			６７５Ａ

審査請求　未請求　請求項の数11　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－339959(P2001－339959)

(22)出願日　平成13年11月５日(2001.11.5)

(71)出願人　598090519
株式会社オープンループ
北海道札幌市清田区北野一条二丁目10番40号

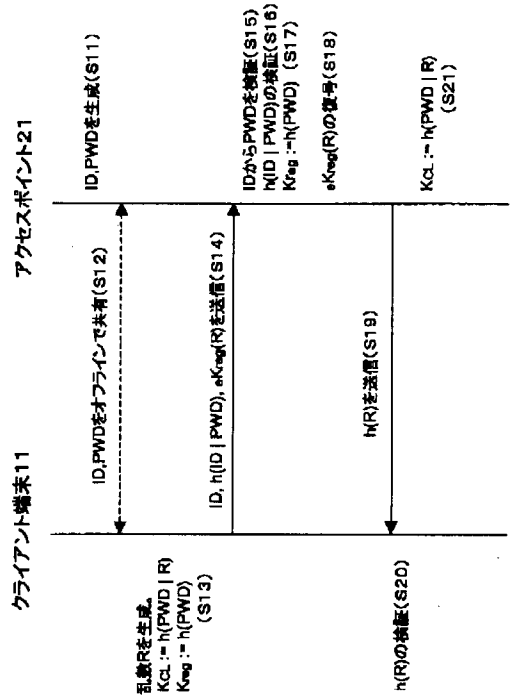
(72)発明者　村上　修一
北海道札幌市清田区北野二条三丁目２番１号　株式会社オープンループ内

(74)代理人　100095407
弁理士　木村　満　（外１名）

Ｆターム(参考)　5J104 AA07 KA02 KA04 KA06 PA07

(54)【発明の名称】　通信システム及び通信方法

(57)【要約】
【課題】　簡単な構成で、高セキュリティ通信を可能とする。
【解決手段】　クライアント端末１１のＩＤとＰＷＤとをオフラインで共有する（Ｓ１１，Ｓ１２）。クライアント端末１１で乱数値Ｒを生成し、Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算して、ＫｒｅｇでＲを暗号化してｅＫｒｅｇ（Ｒ）を求め、アクセスポイント２１に、ＩＤ、ｈ（ＩＤ｜ＰＷＤ）、ｅＫｒｅｇ（Ｒ）を送信する（Ｓ１３，Ｓ１４）。アクセスポイント２１は、受信したＩＤに対応するＰＷＤを求め（Ｓ１５）、ｈ（ＩＤ｜ＰＷＤ）を求め（Ｓ１６）、受信した値と一致した場合に、Ｋｒｅｇを計算し（Ｓ１７）、ＫｒｅｇでｅＫｒｅｇ（Ｒ）を復号してＲを抽出し（Ｓ１８）、Ｒのハッシュ値をクライアント端末１１に送信する（Ｓ１９）。クライアント端末１１は、Ｒのハッシュ値が、受信した値と一致する場合に、認証ＯＫをアクセスポイント２１に通知する。以後、ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を暗号鍵とする。



【特許請求の範囲】
【請求項１】相互に通信を行う第１の装置（１１）と第２の装置（２１）との間で、
前記第１の装置の識別子ＩＤと秘密情報ＰＷＤとを前記第１と第２の装置で共有し、
前記第１の装置において、所定値Ｒを生成し、秘密情報ＰＷＤの一方向関数値Ｋｒｅｇ：＝ｈ（ＰＷＤ）を求め、求めた秘密情報の一方向関数値Ｋｒｅｇを認証用の暗号鍵として用いて、所定値Ｒを暗号化して暗号データｅＫｒｅｇ（Ｒ）を計算し、前記第２の装置に、識別子ＩＤと、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）と、暗号化された所定値ｅＫｒｅｇ（Ｒ）とを送信し、
前記第２の装置は、受信した識別子ＩＤに対応する秘密情報ＰＷＤを検索し、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、これと受信した一方向関数値ｈ（ＩＤ｜ＰＷＤ）と比較し、一致した場合に、認証用の暗号鍵Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算し、この認証用の暗号鍵Ｋｒｅｇを用いて暗号化された所定値ｅＫｒｅｇ（Ｒ）を復号して、所定値Ｒを抽出し、これを一方向性関数で変換した値ｈ（Ｒ）を前記第１の装置に送信し、
前記第１の装置は、所定値Ｒの一方向性関数値ｈ（Ｒ）を求め、これと受信した所定値Ｒの一方向性関数値ｈ（Ｒ）とを比較し、一致する場合に、認証が成立したことを前記第２の装置に通知し、
前記第１の装置は、秘密情報ＰＷＤと所定値Ｒの連結の一方向関数値ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を暗号用の共通鍵ＫＣＬとして求め、
前記第２の装置は、共通鍵ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を計算し、
前記第１の装置と前記第２の装置とは、共通鍵ＫＣＬを暗号鍵として用いて相互に通信を行う、
ことを特徴とする通信方法。
【請求項２】前記第２の装置は、前記第１の装置のアドレスと共通鍵ＫＣＬとを対応付けて格納し、前記第１の装置との通信時に、前記第１の装置のアドレスを判別して、判別したアドレスに対応する共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第１の装置からの受信データを復号化し、前記第１の装置への送信データを暗号化し、
前記第１の装置は、前記第２の装置との通信時に、自己の共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第２の装置からの受信データを復号化し、前記第２の装置への送信データを暗号化する、
ことを特徴とする請求項１に記載の通信方法。
【請求項３】前記第１の装置は、ユーザの識別情報ＰＩＮの一方向関数値Ｋｓａｖｅ：＝ｈ（ＰＩＮ）を計算して保存用の暗号鍵Ｋｓａｖｅとし、この保存用暗号鍵Ｋｓａｖｅにより共通鍵ＫＣＬを暗号化して、暗号化した共通鍵ｅＫｓａｖｅ（ＫＣＬ）を保存し、
前記第２の装置は、前記第１の装置のアドレスと共通鍵とを対応付けて格納し、識別子ＩＤと秘密情報ＰＷＤとを破棄する、
ことを特徴とする請求項１又は２に記載の通信方法。
【請求項４】前記第２の装置で、前記第１の装置の識別子ＩＤと秘密情報ＰＷＤを生成し、生成日時Ｔと共に記憶部に格納し、
前記第２の装置から前記第１の装置に、識別子ＩＤと秘密情報ＰＷＤをオフラインで渡し、前記第１の装置に登録することを特徴とする請求項１、２又は３に記載の通信方法。
【請求項５】前記第２の装置は、
前記第１の装置から受信した識別子を記憶部に検出できなかった場合には、認証不成立とし、
現在日時と生成日時Ｔとの差が設定値以上である場合は認証不成立とし、
前記第２の装置において、識別子ＩＤと秘密情報ＰＷＤの連結の一方向性関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、受信したものと一致しない場合は認証不成立とし、
前記第２の装置は、受信した識別子ＩＤに対応する秘密情報ＰＷＤを検索し、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、これと受信した一方向関数値ｈ（ＩＤ｜ＰＷＤ）と比較し、一致しない場合は認証不成立とし、
前記第１の装置は、所定値Ｒの一方向性関数値ｈ（Ｒ）を求め、これと受信した所定値Ｒの一方向性関数値ｈ（Ｒ）とを比較し、一致しない場合は認証不成立を前記第２の装置に送信する、
ことを特徴とする請求項４に記載の通信方法。
【請求項６】第１の装置（１１）と第２の装置（２１）との間で通信を行う通信システムであって、
前記第１の装置の識別子ＩＤと秘密情報ＰＷＤとを前記第１と第２の装置で共有し、
前記第１の装置は、所定値Ｒを生成し、秘密情報ＰＷＤの一方向関数値Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算し、計算した秘密情報の一方向関数値Ｋｒｅｇを認証用の暗号鍵として用いて、所定値Ｒを暗号化して暗号データｅＫｒｅｇ（Ｒ）を計算し、前記第２の装置に、識別子ＩＤと、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）と、暗号化された所定値ｅＫｒｅｇ（Ｒ）とを送信し、
前記第２の装置は、受信した識別子ＩＤに対応する秘密情報ＰＷＤを検索し、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、これと受信した一方向関数値ｈ（ＩＤ｜ＰＷＤ）とを比較し、一致した場合に、認証用の暗号鍵Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算し、この認証用の暗号鍵Ｋｒｅｇを用いて暗号化された所定値ｅＫｒｅｇ（Ｒ）を復号して、所定値Ｒを抽出し、これを一方向性関数で変換した値ｈ

（Ｒ）を前記第１の装置に送信し、
前記第１の装置は、所定値Ｒの一方向性関数値ｈ（Ｒ）を求め、これと受信した所定値Ｒの一方向性関数値ｈ（Ｒ）とを比較し、一致する場合に、認証が成立したことを前記第２の装置に通知し、
前記第１の装置は、秘密情報ＰＷＤと所定値Ｒの連結の一方向関数値ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を暗号用の共通鍵ＫＣＬとして求めて保存し、
前記第２の装置は、共通鍵ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を計算して保存し、
前記第１の装置と前記第２の装置とは、共通鍵ＫＣＬを暗号鍵として用いて相互に通信を行う、
ことを特徴とする通信システム。
【請求項７】相互に通信を行う第１の装置（１１）と第２の装置（２１）との間で、
前記第１の装置の秘密鍵ＫＣＬを生成し、前記第１の装置のアドレスとこの秘密鍵ＫＣＬのペアを、前記第２の装置にオフラインで通知して登録し、
前記第２の装置は、アイドル時に、自己の秘密鍵ＫＡＰを生成し、
前記第２の装置は、前記第１の装置からの接続要求を受信し、要求元の前記第１の装置のアドレスから前記第１の装置の秘密鍵ＫＣＬを検索し、セッション鍵Ｋを生成し、所定値Ｒとセッション鍵Ｋと自己の秘密鍵ＫＡＰとの連結を前記第１の装置の秘密鍵ＫＣＬにて暗号化して暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を生成して、前記第１の装置に送信し、
前記第１の装置は、自己宛の暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を自己の秘密鍵ＫＣＬにて復号して、所定値Ｒとセッション鍵Ｋと前記第２の装置の秘密鍵ＫＡＰとを抽出し、さらに、抽出した所定値Ｒを前記第２の装置の秘密鍵ＫＡＰで暗号化して暗号データｅＫＡＰ（Ｒ）を生成し、生成した暗号データｅＫＡＰ（Ｒ）を前記第２の装置に送信し、
前記第２の装置は、暗号データｅＫＡＰ（Ｒ）を受信し、これを前記第２の装置の秘密鍵ＫＡＰにて復号して所定値Ｒを抽出し、抽出した所定値Ｒと前記第１の装置に送信した所定値Ｒとを比較し、一致していれば、認証成立と判別し、
前記第１の装置と前記第２の装置は、それぞれ、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを保存し、
以後、前記第１の装置と前記第２の装置は、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを用いて、暗号通信を実行する、
ことを特徴とする通信方法。
【請求項８】前記第２の装置は、前記第１の装置のアドレスと共通鍵ＫＣＬとを対応付けて格納し、
前記第２の装置と個々の前記第１の装置との間で通信を行う場合に、
前記第２の装置は、前記第１の装置のアドレスを判別して、判別したアドレスに対応する共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第１の装置からの受信データを復号化し、前記第１の装置への送信データを暗号化し、前記第１の装置は、前記第２の装置との通信時に、自己の共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第２の装置からの受信データを復号化し、前記第２の装置への送信データを暗号化し、
前記第２の装置から複数の前記第１の装置に共通のデータを送信する場合に、
前記第２の装置は、自己の秘密鍵ＫＡＰを読み出し、読み出した秘密鍵ＫＡＰを用いて、複数の前記第１の装置への送信データを暗号化し、前記第１の装置は、前記第２の装置の秘密鍵ＫＡＰを読み出し、読み出した秘密鍵ＫＡＰを用いて、前記第２の装置からの受信データを復号化する、
ことを特徴とする請求項７に記載の通信方法。
【請求項９】前記第２の装置は、送信対象のデータの送信先アドレスがブロードキャストアドレスの場合、データを前記第２の装置の秘密鍵ＫＡＰで暗号化して送出し、各前記第１の装置は、受信したデータを前記第２の装置の秘密鍵ＫＡＰで復号化し、
宛先アドレスが、記憶部に記憶されている場合、送信対象データを、送信先のアドレスに対応する秘密鍵ＫＣＬで暗号化して送出し、前記第１の装置は、自己宛のデータを、自己の秘密鍵ＫＣＬで復号化し、
宛先アドレスが、記憶部に記憶されていない場合、送信対象データを破棄する、
ことを特徴とする請求項７又は８に記載の通信方法。
【請求項１０】第１の装置（１１）と第２の装置（２１）との間で通信を行う通信システムであって、
前記第１の装置の秘密鍵ＫＣＬを生成し、前記第１の装置のアドレスとこの秘密鍵ＫＣＬのペアを、前記第２の装置にオフラインで通知し、これを記憶部に登録し、
前記第２の装置は、アイドル時に、自己の秘密鍵ＫＡＰを生成し格納し、
前記第２の装置は、前記第１の装置からの接続要求を受信し、要求元の前記第１の装置のアドレスから前記第１の装置の秘密鍵ＫＣＬを検索し、セッション鍵Ｋを生成し、所定値Ｒとセッション鍵Ｋと自己の秘密鍵ＫＡＰとの連結を前記第１の装置の秘密鍵ＫＣＬにて暗号化して暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を生成して、前記第１の装置に送信し、
前記第１の装置は、自己宛の暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を自己の秘密鍵ＫＣＬにて復号して、所定値Ｒとセッション鍵Ｋと前記第２の装置の秘密鍵ＫＡＰとを抽出し、さらに、抽出した所定値Ｒを前記第２の装置の秘密鍵ＫＡＰで暗号化して暗号データｅＫＡＰ（Ｒ）を生成し、生成した暗号データｅＫＡＰ（Ｒ）を

前記第２の装置に送信し、
前記第２の装置は、暗号データｅＫＡＰ（Ｒ）を受信し、これを秘密鍵ＫＡＰにて復号して所定値Ｒを抽出し、抽出した所定値Ｒと前記第１の装置に送信した送った所定値Ｒと比較し、一致していれば、認証成立と判別し、
前記第１の装置と前記第２の装置は、それぞれ、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを保存し、
以後、前記第１の装置と前記第２の装置は、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを用いて、暗号通信を実行する、ことを特徴とする通信システム。
【請求項１１】コンピュータを請求項５又は１０の第１の装置又は第２の装置として動作させるためのコンピュータプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号通信システムと方法に関する。
【０００２】
【従来の技術】安価で簡単な無線ＬＡＮ構築デバイスとして、ＩＥＥＥ８０２．１１ｂ準拠の無線ＬＡＮが普及している。
【０００３】
【発明が解決しようとする課題】しかし、ＩＥＥＥ８０２．１１ｂには、「セキュリティ」上の問題が指摘されている。即ち、ＩＥＥＥ８０２．１１ｂのセキュリティプロトコルＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｃｙ　Ｐｒｉｖａｃｙ）は脆弱であり、通信のセキュリティが維持されない危険がある。同様の問題は、有線での通信にも該当し、より簡便で高信頼の暗号通信システム、暗号通信プロトコルなどが望まれている。
【０００４】本発明は、上述した事情に鑑みてなされたもので、信頼性の高い通信を行うことが可能なシステムと方法を提供することを目的とする。また、この発明は簡単な構成で、高セキュリティな通信を可能とすることを他の目的とする。
【０００５】
【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点に係る、通信方法は、相互に通信を行う第１の装置（１１）と第２の装置（２１）との間で、前記第１の装置の識別子ＩＤと秘密情報ＰＷＤとを前記第１と第２の装置で共有し、前記第１の装置において、所定値Ｒを生成し、秘密情報ＰＷＤの一方向関数値Ｋｒｅｇ：＝ｈ（ＰＷＤ）を求め、求めた秘密情報の一方向関数値Ｋｒｅｇを認証用の暗号鍵として用いて、所定値Ｒを暗号化して暗号データｅＫｒｅｇ（Ｒ）を計算し、前記第２の装置に、識別子ＩＤと、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）と、暗号化された所定値ｅＫｒｅｇ（Ｒ）とを送信し、前記第２の装置は、受信した識別子ＩＤに対応する秘密情報ＰＷＤを検索し、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、これと受信した一方向関数値ｈ（ＩＤ｜ＰＷＤ）と比較し、一致した場合に、認証用の暗号鍵Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算し、この認証用の暗号鍵Ｋｒｅｇを用いて暗号化された所定値ｅＫｒｅｇ（Ｒ）を復号して、所定値Ｒを抽出し、これを一方向性関数で変換した値ｈ（Ｒ）を前記第１の装置に送信し、前記第１の装置は、所定値Ｒの一方向性関数値ｈ（Ｒ）を求め、これと受信した所定値Ｒの一方向性関数値ｈ（Ｒ）とを比較し、一致する場合に、認証が成立したことを前記第２の装置に通知し、前記第１の装置は、秘密情報ＰＷＤと所定値Ｒの連結の一方向関数値ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を暗号用の共通鍵ＫＣＬとして求め、前記第２の装置は、共通鍵ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を計算し、前記第１の装置と前記第２の装置とは、共通鍵ＫＣＬを暗号鍵として用いて相互に通信を行う、ことを特徴とする。
【０００６】例えば、前記第２の装置は、前記第１の装置のアドレスと共通鍵ＫＣＬとを対応付けて格納し、前記第１の装置との通信時に、前記第１の装置のアドレスを判別して、判別したアドレスに対応する共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第１の装置からの受信データを復号化し、前記第１の装置への送信データを暗号化し、前記第１の装置は、前記第２の装置との通信時に、自己の共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第２の装置からの受信データを復号化し、前記第２の装置への送信データを暗号化する。
【０００７】前記第１の装置は、ユーザの識別情報ＰＩＮの一方向関数値Ｋｓａｖｅ：＝ｈ（ＰＩＮ）を計算して保存用の暗号鍵Ｋｓａｖｅとし、この保存用暗号鍵Ｋｓａｖｅにより共通鍵ＫＣＬを暗号化して、暗号化した共通鍵ｅＫｓａｖｅ（ＫＣＬ）を保存し、前記第２の装置は、前記第１の装置のアドレスと共通鍵とを対応付けて格納し、識別子ＩＤと秘密情報ＰＷＤとを破棄する、ようにしてもよい。
【０００８】前記第２の装置で、前記第１の装置の識別子ＩＤと秘密情報ＰＷＤを生成し、生成日時Ｔと共に記憶部に格納し、前記第２の装置から前記第１の装置に、識別子ＩＤと秘密情報ＰＷＤをオフラインで渡し、前記第１の装置に登録するようにしてもよい。
【０００９】この場合において、前記第２の装置は、前記第１の装置から受信した識別子を記憶部に検出できなかった場合には、認証不成立とし、現在日時と生成日時Ｔとの差が設定値以上である場合は認証不成立とし、前記第２の装置において、識別子ＩＤと秘密情報ＰＷＤの連結の一方向性関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、受信したものと一致しない場合は認証不成立とし、前記第

２の装置は、受信した識別子ＩＤに対応する秘密情報ＰＷＤを検索し、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、これと受信した一方向関数値ｈ（ＩＤ｜ＰＷＤ）と比較し、一致しない場合は認証不成立としてもよい。また、前記第１の装置は、所定値Ｒの一方向性関数値ｈ（Ｒ）を求め、これと受信した所定値Ｒの一方向性関数値ｈ（Ｒ）とを比較し、一致しない場合は認証不成立を前記第２の装置に送信するようにしてもよい。

【００１０】上記目的を達成するため、本発明の第２の観点に係る、通信システムは、第１の装置（１１）と第２の装置（２１）との間で通信を行う通信システムであって、前記第１の装置の識別子ＩＤと秘密情報ＰＷＤとを前記第１と第２の装置で共有し、前記第１の装置は、所定値Ｒを生成し、秘密情報ＰＷＤの一方向関数値Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算し、計算した秘密情報の一方向関数値Ｋｒｅｇを認証用の暗号鍵として用いて、所定値Ｒを暗号化して暗号データｅＫｒｅｇ（Ｒ）を計算し、前記第２の装置に、識別子ＩＤと、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）と、暗号化された所定値ｅＫｒｅｇ（Ｒ）とを送信し、前記第２の装置は、受信した識別子ＩＤに対応する秘密情報ＰＷＤを検索し、識別子ＩＤと秘密情報ＰＷＤとの連結の一方向関数値ｈ（ＩＤ｜ＰＷＤ）を計算し、これと受信した一方向関数値ｈ（ＩＤ｜ＰＷＤ）とを比較し、一致した場合に、認証用の暗号鍵Ｋｒｅｇ：＝ｈ（ＰＷＤ）を計算し、この認証用の暗号鍵Ｋｒｅｇを用いて暗号化された所定値ｅＫｒｅｇ（Ｒ）を復号して、所定値Ｒを抽出し、これを一方向性関数で変換した値ｈ（Ｒ）を前記第１の装置に送信し、前記第１の装置は、所定値Ｒの一方向性関数値ｈ（Ｒ）を求め、これと受信した所定値Ｒの一方向性関数値ｈ（Ｒ）とを比較し、一致する場合に、認証が成立したことを前記第２の装置に通知し、前記第１の装置は、秘密情報ＰＷＤと所定値Ｒの連結の一方向関数値ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を暗号用の共通鍵ＫＣＬとして求め、前記第２の装置は、共通鍵ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を計算し、前記第１の装置と前記第２の装置とは、共通鍵ＫＣＬを暗号鍵として用いて相互に通信を行う、ことを特徴とする。

【００１１】上記目的を達成するため、本発明の第３の観点に係る、通信方法は、相互に通信を行う第１の装置（１１）と第２の装置（２１）との間で、前記第１の装置の秘密鍵ＫＣＬを生成し、前記第１の装置のアドレスとこの秘密鍵ＫＣＬのペアを、前記第２の装置にオフラインで通知して登録し、前記第２の装置は、アイドル時に、自己の秘密鍵ＫＡＰを生成し、前記第２の装置は、前記第１の装置からの接続要求を受信し、要求元の前記第１の装置のアドレスから前記第１の装置の秘密鍵ＫＣＬを検索し、セッション鍵Ｋを生成し、所定値Ｒとセッション鍵Ｋと自己の秘密鍵ＫＡＰとの連結を前記第１の装置の秘密鍵ＫＣＬにて暗号化して暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を生成して、前記第１の装置に送信し、前記第１の装置は、自己宛の暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を自己の秘密鍵ＫＣＬにて復号して、所定値Ｒとセッション鍵Ｋと前記第２の装置の秘密鍵ＫＡＰとを抽出し、さらに、抽出した所定値Ｒを前記第２の装置の秘密鍵ＫＡＰで暗号化して暗号データｅＫＡＰ（Ｒ）を生成し、生成した暗号データｅＫＡＰ（Ｒ）を前記第２の装置に送信し、前記第２の装置は、暗号データｅＫＡＰ（Ｒ）を受信し、これを前記第２の装置の秘密鍵ＫＡＰにて復号して所定値Ｒを抽出し、抽出した所定値Ｒと前記第１の装置に送信した所定値Ｒとを比較し、一致していれば、認証成立と判別し、前記第１の装置と前記第２の装置は、それぞれ、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを保存し、以後、前記第１の装置と前記第２の装置は、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを用いて、暗号通信を実行する、ことを特徴とする。

【００１２】例えば、前記第２の装置は、前記第１の装置のアドレスと共通鍵ＫＣＬとを対応付けて格納し、前記第２の装置と個々の前記第１の装置との間で通信を行う場合に、前記第２の装置は、前記第１の装置のアドレスを判別して、判別したアドレスに対応する共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第１の装置からの受信データを復号化し、前記第１の装置への送信データを暗号化し、前記第１の装置は、前記第２の装置との通信時に、自己の共通鍵ＫＣＬを読み出し、読み出した共通鍵ＫＣＬを用いて、前記第２の装置からの受信データを復号化し、前記第２の装置への送信データを暗号化し、前記第２の装置から複数の前記第１の装置に共通のデータを送信する場合に、前記第２の装置は、自己の秘密鍵ＫＡＰを読み出し、読み出した秘密鍵ＫＡＰを用いて、複数の前記第１の装置への送信データを暗号化し、前記第１の装置は、前記第２の装置の秘密鍵ＫＡＰを読み出し、読み出した秘密鍵ＫＡＰを用いて、前記第２の装置からの受信データを復号化する。

【００１３】例えば、前記第２の装置は、送信対象のデータの送信先アドレスがブロードキャストアドレスの場合、データを前記第２の装置の秘密鍵ＫＡＰで暗号化して送出し、各前記第１の装置は、受信したデータを前記第２の装置の秘密鍵ＫＡＰで復号化し、宛先アドレスが、記憶部に記憶されている場合、送信対象データを、送信先のアドレスに対応する秘密鍵ＫＣＬで暗号化して送出し、前記第１の装置は、自己宛のデータを、自己の秘密鍵ＫＣＬで復号化し、宛先アドレスが、記憶部に記憶されていない場合、送信対象データを破棄する。

【００１４】上記目的を達成するため、本発明の第４の観点に係る、通信システムは、第１の装置（１１）と第２の装置（２１）との間で通信を行う通信システムであ

って、前記第１の装置の秘密鍵ＫＣＬを生成し、前記第１の装置のアドレスとこの秘密鍵ＫＣＬのペアを、前記第２の装置にオフラインで通知し、これを記憶部に登録し、前記第２の装置は、アイドル時に、自己の秘密鍵ＫＡＰを生成し格納し、前記第２の装置は、前記第１の装置からの接続要求を受信し、要求元の前記第１の装置のアドレスから前記第１の装置の秘密鍵ＫＣＬを検索し、セッション鍵Ｋを生成し、所定値Ｒとセッション鍵Ｋと自己の秘密鍵ＫＡＰとの連結を前記第１の装置の秘密鍵ＫＣＬにて暗号化して暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を生成して、前記第１の装置に送信し、前記第１の装置は、自己宛の暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を自己の秘密鍵ＫＣＬにて復号して、所定値Ｒとセッション鍵Ｋと前記第２の装置の秘密鍵ＫＡＰとを抽出し、さらに、抽出した所定値Ｒを前記第２の装置の秘密鍵ＫＡＰで暗号化して暗号データｅＫＡＰ（Ｒ）を生成し、生成した暗号データｅＫＡＰ（Ｒ）を前記第２の装置に送信し、前記第２の装置は、暗号データｅＫＡＰ（Ｒ）を受信し、これを秘密鍵ＫＡＰにて復号して所定値Ｒを抽出し、抽出した所定値Ｒと前記第１の装置に送信した送った所定値Ｒと比較し、一致していれば、認証成立と判別し、前記第１の装置と前記第２の装置は、それぞれ、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを保存し、以後、前記第１の装置と前記第２の装置は、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを用いて、暗号通信を実行する、ことを特徴とする。

【００１５】コンピュータを、上記第１の装置又は第２の装置として動作させ、或いは、コンピュータに、上記第１の装置又は第２の装置の動作を実行させるためのプログラムを作成・配布などしてもよい。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態に係る通信システムと通信方法を図面を参照して説明する。

【００１７】この実施の形態に係る通信システムは、図１に示すように、複数のクライアント端末（ユーザ端末）１１（１１１～１１ｎ）と、クライアント端末１１との間で無線ＬＡＮ４１を構成するアクセスポイント（サーバ）２１と、アクセスポイント２１に有線LAN４２などを介して接続され、外部のネットワークに接続されたゲートウエイサーバ３１とより構成される。

【００１８】各クライアント端末１１は、パーソナルコンピュータ、ワークステーションなどから構成され、図２に示すように、記憶部１１１と、入力部１１２と、表示部１１３と処理部１１４とを備え、無線ＬＡＮカード１２が装着されている。

【００１９】記憶部１１１は、ＲＡＭ、ＲＯＭ、ハードディスクなどから構成され、様々なデータやプログラムを記憶する。この実施の形態においては、自端末の識別子ＩＤ、パスワードＰＷＤ、乱数値Ｒ、秘密鍵ＫＣＬ、登録用鍵Ｋｒｅｇ、保存用鍵Ｋｓａｖｅ等のデータ、認証プログラム、暗号化プログラム、アプリケーションプログラム、通信プログラムなどの動作プログラムを記憶する。

【００２０】入力部１１２は、キーボード、マウス、記録媒体入出力装置などを備え、様々なデータや指示を処理部１１４に供給する。表示部１１３は、様々な情報を表示する。

【００２１】処理部１１４は、プロセッサなどを備え、記憶部１１１に記憶された動作プログラムに従って動作する。この実施の形態例においては、認証処理、暗号通信処理を実行する。また、処理部１１４は、タイマを備えている。

【００２２】無線ＬＡＮカード１２は、いわゆるＰＣカードとして構成され、クライアント端末１１に装着され、処理部１１４から供給される送信データを無線信号に変換してアクセスポイント２１に送信し、アクセスポイント２１が送信する無線信号を受信して復号し、処理部１１４に提供する。無線ＬＡＮカード１２内には、そのカードを識別するための固有のＭＡＣ（Ｍａｃｈｉｎｅ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスが記憶されている。

【００２３】アクセスポイント２１は、複数のクライアント端末１１との間で無線ＬＡＮ４１を構成し、無線ＬＡＮ４１と有線ＬＡＮ４２ととの間でデータの伝達するためのものであり、図３に示すように、無線ＩＦ（インタフェース）２１１、有線ＩＦ（インタフェース）２１２、記憶部２１３と、データベース２１４と、入力部２１５と、表示部２１６と、処理部２１７とを備える。

【００２４】無線ＩＦ２１１は、クライアント端末１１からの無線信号を受信して復調し、処理部２１７に提供し、また、処理部２１７から提供される送信データを無線信号に変換して無線送信する。

【００２５】有線ＩＦ２１２は、有線ＬＡＮ４２上の信号を処理部２１７に提供し、また、処理部２１７から提供される信号を有線ＬＡＮ４２上に送出する。

【００２６】記憶部２１３は、ＲＡＭ、ＲＯＭ、ハードディスクなどから構成され、様々なデータやプログラムを記憶する。この実施の形態においては、乱数値Ｒ、秘密鍵ＫＣＬ、登録用鍵Ｋｒｅｇ、保存用鍵Ｋｓａｖｅ等のデータ、認証プログラム、暗号化プログラム、アプリケーションプログラム、通信プログラムなどの動作プログラムを記憶する。

【００２７】データベース（ＤＢ）２１４は、図４に示すように、登録情報ＤＢとクライアント鍵ＤＢとを含む。登録情報ＤＢは、各クライアント端末１１の識別子ＩＤと、パスワード（事前設定秘密情報）ＰＷＤと、識別子ＩＤとパスワードＰＷＤとの生成日時Ｔとを対応付けて記憶する。クライアント鍵ＤＢは、クライアント端末１１に装着された無線ＬＡＮカード１２のＭＡＣアド

レスとクライアント鍵（秘密暗号鍵；共通鍵）ＫＣＬとを対応付けて記憶する。

【００２８】図３の入力部２１５は、キーボード、マウス、記録媒体入出力装置などを備え、様々なデータや指示を処理部２１７に供給する。表示部２１６は、様々な情報を表示する。

【００２９】処理部２１７は、プロセッサなどを備え、記憶部に記憶された動作プログラムに従って動作する。特に、この実施の形態においては、クライアント端末１１の認証処理などを含む無線暗号通信処理と、無線LAN４１と有線LAN４２との間のデータのブリッジ処理を実行する。処理の詳細については、後述する。

【００３０】図１のゲートウエイサーバ３１は、有線ＬＡＮ４２に接続され、インターネットインＩＮ等の外部のネットワークに接続されている。

【００３１】次に、上記構成を有する通信システムの動作を説明する。この通信システムにおいて、クライアント端末１１とアクセスポイント２１との間で構築される無線ＬＡＮ４１を介してデータを受信するためには、図５に示すように、事前登録と相互認証の手順を踏む必要がある。

【００３２】（１）　クライアント端末１１のアクセスポイント２１への事前登録

無線ＬＡＮ４１に新たにクライアント端末１１を接続する場合、システムの管理者は、アクセスポイント２１で、ＩＤとパスワードＰＷＤとを事前に生成し（ステップＳ１１）、生成日時Ｔと共に登録情報ＤＢに図４（ａ）に示すように登録する。

【００３３】生成された識別子ＩＤとパスワードＰＷＤとは、オフラインでそのクライアント端末１１に通知され、例えば、入力部２１３から入力され、記憶部１１１に登録される（ステップＳ１２）。これにより、新たなクライアント端末１１の識別子ＩＤとパスワードＰＷＤとが、クライアント端末１１とアクセスポイント２１との間で共有される。

【００３４】（２）　クライアント端末１１とアクセスポイント２１の相互認証と暗号鍵の交換

ａ）　クライアント端末１１は、無線ＬＡＮ４１を介して通信を行いたい場合には、アクセスポイント２１に接続を要求する。この要求に応答して、アクセスポイント２１は、オープン認証により、クライアント端末１１との間で無線通信による接続を一旦確立する。

【００３５】ｂ）　次に、クライアント端末１１の処理部１１４は、乱数プログラムを実行して、乱数値Ｒを生成する（なお、乱数が望ましいが、任意の定数でもよい）。さらに、処理部１１４は、所定のハッシュ関数ｈ（　）により、数１により定義されるパスワードＰＷＤと乱数値Ｒとの連結のハッシュ値と、パスワードＰＷＤのハッシュ値とを計算し、クライアント端末１１のクライアント鍵ＫＣＬと、登録用鍵Ｋｒｅｇとし、記憶部１１に格納する（ステップＳ１３）。なお、クライアント鍵ＫＣＬは、クライアント１１とアクセスポイント２１とに共通の秘密鍵であり、登録用鍵Ｋｒｅｇは、認証処理にのみ使用される共通鍵である。

【数１】ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）

Ｋｒｅｇ：＝ｈ（ＰＷＤ）

第１の装置（１１）と第２の装置（２１）との間で通信を行う通信システムであって、前記第１の装置の秘密鍵ＫＣＬを生成し、前記第１の装置のアドレスとこの秘密鍵ＫＣＬのペアを、前記第２の装置にオフラインで通知し、これを記憶部に登録し、前記第２の装置は、アイドル時に、自己の秘密鍵ＫＡＰを生成し格納し、前記第２の装置は、前記第１の装置からの接続要求を受信し、要求元の前記第１の装置のアドレスから前記第１の装置の秘密鍵ＫＣＬを検索し、セッション鍵Ｋを生成し、所定値Ｒとセッション鍵Ｋと自己の秘密鍵ＫＡＰとの連結を前記第１の装置の秘密鍵ＫＣＬにて暗号化して暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を生成して、前記第１の装置に送信し、前記第１の装置は、自己宛の暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を自己の秘密鍵ＫＣＬにて復号して、所定値Ｒとセッション鍵Ｋと前記第２の装置の秘密鍵ＫＡＰとを抽出し、さらに、抽出した所定値Ｒを前記第２の装置の秘密鍵ＫＡＰで暗号化して暗号データｅＫＡＰ（Ｒ）を生成し、生成した暗号データｅＫＡＰ（Ｒ）を前記第２の装置に送信し、前記第２の装置は、暗号データｅＫＡＰ（Ｒ）を受信し、これを秘密鍵ＫＡＰにて復号して所定値Ｒを抽出し、抽出した所定値Ｒと前記第１の装置に送信した送った乱数値Ｒと比較し、一致していれば、認証成立と判別し、前記第１の装置と前記第２の装置は、それぞれ、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを保存し、以後、前記第１の装置と前記第２の装置は、前記第１の装置の秘密鍵ＫＣＬと前記第２の装置の秘密鍵ＫＡＰとを用いて、暗号通信を実行する、

【００３６】ｃ）　次に、識別子ＩＤとパスワードＰＷＤとの連結のハッシュ値ｈ（ＩＤ｜ＰＷＤ）と、乱数値Ｒの登録用鍵Ｋｒｅｇによる暗号化データｅＫｒｅｇ（Ｒ）とを生成して、記憶部１１１に一時的に格納する。なお、識別子ＩＤとパスワードＰＷＤとの連結のハッシュ値ｈ（ＩＤ｜ＰＷＤ）は、送信段階までに、アクセスポイント２１又はクライアント端末１１のいずれかで計算されていればよい。

【００３７】ｄ）　続いて、クライアント端末１１は、自己の識別子ＩＤと、ハッシュ値ｈ（ＩＤ｜ＰＷＤ）、及び暗号データｅＫｒｅｇ（Ｒ）をアクセスポイント２１に送信する（ステップＳ１４）。

【００３８】ｅ）　アクセスポイント２１の処理部２１７は、無線ＩＦ２１１を介してこれらのデータを受信し、一旦、記憶部２１３に格納する。続いて、受信した識別子ＩＤをキーに登録情報ＤＢを検索する。

【００３９】ｆ）　この検索処理おいて、受信した識別子ＩＤが、登録情報ＤＢに登録されていない場合、不正アクセスであると判断して、不正アクセスエラーを返送し、以後、そのクライアント端末１１との接続を切断する（ステップＳ１５）。一方、その識別子ＩＤが、登録情報ＤＢに登録されている場合には、対応するパスワードＰＷＤと生成日時Ｔを読み出す。

【００４０】ｇ）　次に、読み出した生成日時Ｔと現在日時との差を求め、それが基準値以上であるか否かを判別する。

ｇ－１）　生成日時Ｔと現在日時との差差が基準値を越えている場合、即ち、登録から長期間経過している場合には、登録タイムアウトをクライアント端末１１に無線ＩＦ２１１を介して返信する。クライアント端末１１の処理部１１４は、これを無線LANカード１２を介して受信し、表示部に１１３に、再登録すべき旨のメッセージを表示させる。

【００４１】ｇ－２）　一方、生成日時Ｔと現在日時との差が基準値未満の場合、即ち、登録タイムアウトに相当しない場合には、処理部２１７は、ハッシュ値ｈ（ＩＤ｜ＰＷＤ）を検証する（ステップＳ１６）。即ち、処理部２１７は、受信した識別子ＩＤと登録情報ＤＢから読み出したパスワードＰＷＤとの連結のハッシュ値ｈ（ＩＤ｜ＰＷＤ）を計算し、クライアント端末１１より受信したハッシュ値ｈ（ＩＤ｜ＰＷＤ）と一致するか否かを判別する。一致しないと判別した場合には、処理部２１７は、クライアント端末１１にチャレンジ失敗を返送し、接続を切断する。

【００４２】ｈ）　一方、計算したハッシュ値ｈ（ＩＤ｜ＰＷＤ）と受信したハッシュ値ｈ（ＩＤ｜ＰＷＤ）とが一致すると判別した場合には、処理部２１７は、登録用鍵Ｋｒｅｇ（：＝ｈ（ＰＷＤ））を計算する（ステップＳ１７）。

【００４３】次に、処理部２１７は、生成した登録用鍵Ｋｒｅｇを用いて、受信した乱数値Ｒの暗号化データｅＫｒｅｇ（Ｒ）を復号し、クライアント端末１１が先に発生させた乱数値Ｒを抽出する（ステップＳ１８）。

【００４４】ｉ）　処理部２１７は、抽出した乱数値Ｒのハッシュ値ｈ（Ｒ）を計算し、これをクライアント端末１１に送信する（ステップＳ１９）。

【００４５】ｊ）　次に、クライアント端末１１の処理部１１４は、乱数値Ｒのハッシュ値ｈ（Ｒ）を検証する（ステップＳ２０）。即ち、処理部１１４は、記憶部１１１に記憶している乱数値Ｒのハッシュ値ｈ（Ｒ）を計算し、これと、アクセスポイント２１より受信したハッシュ値ｈ（Ｒ）とを比較する。処理部１１４は、両ハッシュ値が、一致しない場合は「認証不成立（ＮＧ）」をアクセスポイント２１に返送し、接続を切断する。一方、一致すると判断した場合には、「認証成功（ＯＫ）」をアクセスポイント２１に返送する。

【００４６】ｋ）　認証成功の通知に応答して、アクセスポイント２１の処理部２１７は、クライアント鍵ＫＣＬ：＝ｈ（ＰＷＤ｜Ｒ）を計算し（ステップＳ２１）、無線通信のヘッダ情報に含まれているＭＡＣアドレスを用いて、｛ＭＡＣアドレス、ＫＣＬ｝をデータベース２１４のクライアント鍵ＤＢに登録する。続いて、記憶部２１３上の識別子ＩＤとパスワードＰＷＤを破棄する。

【００４７】ｌ）　クライアント端末１１の処理部１１４は、認証成功を送信した後、ユーザが入力部１１２から、例えば、認証用ＩＣカード等に記録されているユーザのＰＩＮ（個人識別情報）を入力する。処理部１１４は、入力したＰＩＮのハッシュ値：＝ｈ（ＰＩＮ）を計算して、保存用鍵Ｋｓａｖｅとする。処理部１１４は、この保存用鍵Ｋｓａｖｅを用いて、クライアント鍵ＫＣＬを暗号化して、暗号化されたクライアント鍵ｅＫｓａｖｅ（ＫＣＬ）を記憶部１１１に保存する。

【００４８】以上の比較的簡単な手順で、クライアント端末１１とアクセスポイント２１との間の相互認証と暗号鍵の交換が安全に完了し、無線暗号チャネルが確立される。

【００４９】例えば、アクセスポイント２１からクライアント端末１１に、有線ＬＡＮ側から有線ＩＦ２１２を介して受け取ったパケットを無線ＬＡＮ側に送信する場合には、次の処理を行う。

【００５０】まず、受信したパケットの宛先のＭＡＣアドレスを判別し、このＭＡＣアドレスがクライアント鍵データベースに登録されているか否かを判別する。登録されていると判別した場合には、そのＭＡＣアドレスがテーブルに存在する場合、そのＭＡＣアドレスに対応するクライアント鍵ＫＣＬを読み出し、パケットのパケットヘッダを除く部分（ペイロード）をクライアント鍵ＫＣＬで暗号化して、無線ＩＦ２１１から送出する。

【００５１】各クライアント端末１１の処理部１１４は、無線情報を無線通信装置１２を介して取り込む。処理部１１４は、使用者のＰＩＮのハッシュ値ｈ（ＰＩＮ）を求めて、保存用鍵K_{save}を求め、この保存用鍵K_{save}を用いて、記憶部１１１に格納されている暗号化されたクライアント鍵ｅＫｓａｖｅ（ＫＣＬ）を復号する。処理部１１４は、復号化したクライアント鍵ＫＣＬを用いて、自己宛のパケットのペイロード部分を復号化し、記憶部１１１に記憶する。

【００５２】一方、無線通信装置１２は、ヘッダに含まれているＭＡＣアドレスが自己のＭＡＣアドレスと異なる場合には、これを破棄する。これにより、パケットが自己宛で、自己のクライアント鍵ＫＣＬで暗号化されたパケットのみを受信することになる。

【００５３】一方、アクセスポイント２１は、送信対象パケットのＭＡＣアドレスがクライアント鍵ＤＢに存在しないと判断した場合、そのパケットを破棄する。

【００５４】クライアント端末１１からアクセスポイン

ト２１に対してパケットを送出する際には、処理部１１４は、ユーザのＰＩＮから、保存用鍵Ｋｓａｖｅを生成し、この保存用鍵Ｋｓａｖｅでクライアント鍵ＫＣＬを復号化し、パケットの情報格納部分（ペイロード）を復号化したクライアント鍵ＫＣＬで暗号化して、無線ＬＡＮカード１２から送出する。

【００５５】アクセスポイント２１の処理部２１７は、無線信号を無線ＩＦ２１１を介して一旦取り込み、ヘッダ情報から送信元のマックアドレスを判別し、これに対応するクライアント鍵ＫＣＬを、クライアント鍵ＤＢから読み出し、ペイロード部分を復号化する。アクセスポイント２１は、必要ならば、これを有線ＬＡＮ用の暗号化アルゴリズムで暗号化した後、有線ＬＡＮにパケットを送出する。

【００５６】（３）　通信の切断

アクセスポイント２１の管理下にクライアント端末１１が存在しなくなったときは、アクセスポイント２１は、接続を切断し、クライアントからの接続要求を待機する。

【００５７】以上説明したように、この通信システムは、比較的簡単な手順で、クライアント端末１１とアクセスポイント２１との間の相互認証と暗号鍵の交換を安全に行うことができる。共通鍵暗号をベースに設計されている。このため、公開鍵方式を用いる場合と比較して、処理速度を高めることが可能となる。

【００５８】また、各クライアント端末１１の秘密鍵ＫＣＬをアクセスポイント２１に登録し、それを認証処理で用いているため、なりすましを防止できる。

【００５９】（第２の実施の形態）以下、この発明の実施の形態に係る通信システムの第２の実施の形態を説明する。

【００６０】この実施の形態のシステムの基本構成は、第１の実施の形態のシステムの構成と実質的に同一であり、以下、特徴点である通信プロトコルを中心に説明する。

【００６１】（１）　クライアントの登録

まず、無線ＬＡＮカード１２がインストールされたクライアント端末１１上で、処理部１１４は、クライアントの秘密鍵ＫＣＬを生成する。

【００６２】次に、無線ＬＡＮカード１２のＭＡＣアドレスとこの共通鍵ＫＣＬのペアを、アクセスポイント２１にオフラインで送信する。アクセスポイント２１は、この対をデータベース２１４に登録する。

【００６３】（２）　アクセスポイント鍵の生成

アクセスポイント２１の処理部２１７は、そのアイドル時（通信を行っているクライアント端末１１が存在しないとき）に、アクセスポイント２１の秘密鍵ＫＡＰを、動的に生成し、記憶部２１３に格納する。

【００６４】（３）　クライアント端末１１の認証

アクセスポイント２１は、クライアント端末１１からの接続要求を受信した時には、次の手順にて鍵交換、および、認証を行う。

【００６５】ａ）．　クライアント端末１１はアクセスポイント２１に対して接続要求を送信する。

【００６６】ｂ）．　アクセスポイント２１の処理部２１７は接続要求を受信し、データベース２１４をアクセスし、クライアント端末１１のＭＡＣアドレスからクライアント鍵ＫＣＬを検索する。

【００６７】ｃ）．　アクセスポイント２１の処理部２１７はセッション鍵Ｋをランダムに生成する。

ｄ）．　アクセスポイント２１の処理部２１７は、乱数値Ｒとセッション鍵Ｋとアクセスポイント鍵ＫＡＰとの連結をクライアント鍵ＫＣＬにて暗号化して暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を生成する。

【００６８】ｅ）．　アクセスポイント２１の処理部２１７は、無線ＩＦ２１１を介して、暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）をクライアント端末１１に送信する。

【００６９】ｆ）．　クライアント端末１１の処理部１１４は、無線LANカード１２を介して、自己宛の暗号データｅＫＣＬ（Ｒ｜Ｋ｜ＫＡＰ）を自己のクライアント鍵ＫＣＬにて復号して乱数値Ｒ、セッション鍵Ｋ、アクセスポイント鍵ＫＡＰを抽出する。

【００７０】ｇ）．　クライアント端末１１の処理部１１４は、乱数値Ｒをアクセスポイント鍵ＫＡＰで暗号化して暗号データｅＫＡＰ（Ｒ）を生成する。

【００７１】ｈ）．　クライアント端末１１の処理部１１４は、生成した暗号化データｅＫＡＰ（Ｒ）をアクセスポイント２１に送信する。

【００７２】ｉ）．　アクセスポイント２１の処理部２１７は、無線ＩＦ２１１を介して暗号化データｅＫＡＰ（Ｒ）を受信し、これをアクセスポイント鍵ＫＡＰにて復号して乱数値Ｒを抽出する。

【００７３】ｊ）．　アクセスポイント２１は、抽出した乱数値Ｒと先に生成した乱数値Ｒとを比較し、一致すれば、「認証成功（ＯＫ）」と判断する。

【００７４】このようにして、クライアント端末１１の認証が成功した後、クライアント端末１１とアクセスポイント２１の間では、無線暗号通信が実行される。

【００７５】例えば、アクセスポイント２１が有線ＬＡＮ４２側から受け取ったパケットを無線ＬＡＮ４１側に送信する際には、処理部２１７は、ＭＡＣアドレスの値に従って以下の処理を行う。

【００７６】ａ）．　まず、制御部２１７は、有線ＩＦ２１２を介して受信したパケットの送信先アドレスがブロードキャストアドレスの場合、パケットのペイロードをアクセスポイント鍵ＫＡＰで暗号化して無線ＩＦ２１１に送出する。各クライアント端末１１は、パケットを受信し、宛先アドレスがブロードキャストアドレスであることを判別し、記憶部１１１に格納しておいたアクセ

スポイント鍵ＫＡＰでペイロードを復号化する。

【００７７】ｂ）．　制御部２１７は、有線ＩＦ２１２を介して受信したパケットの送信先アドレスが、ＭＡＣアドレスの場合、その宛先アドレスが、データベース２１４に登録されているか否かを判別する。登録されている場合には、そのＭＡＣアドレスに対応するクライアント鍵ＫＣＬを読み出し、そのパケットのペイロードをクライアント鍵ＫＣＬで暗号化して無線ＩＦ２１１に送出する。各クライアント端末１１は、自己宛のパケットを判別し、記憶部１１１に格納しておいたクライアント鍵ＫＣＬでペイロードを復号化する。

【００７８】ｃ）．　宛先アドレスがデータベース２１４に登録されていない場合、処理部２１７は、そのパケットを破棄する。

【００７９】一方、クライアント端末１１からアクセスポイント２１にデータを送信する場合には、各クライアント端末１１の処理部１１４は、パケットのペイロードを自己のクライアント鍵ＫＣＬで暗号化して無線LANカード１２に送出する。アクセスポイント２１は、送信元を送信元アドレスから判別し、これに対応するクライアント鍵ＫＣＬをデータベース２１４上のテーブルから読み出し、パケットのペイロードをクライアント鍵ＫＣＬで復号化する。

【００８０】この第２の実施の形態の通信システムも、共通鍵暗号をベースに設計されているため、処理速度を高くすることができる。また、クライアントの秘密鍵を予め登録し、それを認証処理で用いているため、なりすましを予防できる。また、アクセスポイントの鍵を動的に生成して、クライアント端末と鍵交換を行っており、ＷＥＰの弱点であるＩＶコリジョンによる脆弱性を回避できる。

【００８１】なお、この発明は上記実施の形態に限定されず、種々の変形及び応用が可能である。例えば、上記第１と第２の実施の形態は、基本アルゴリズムとして強力なソリューションを例示しているが、必要に応じて簡略化することも可能である。逆に、認証の際に、他の検証要件を追加してもよい。この発明において、「認証成功」とは、他の要件又は条件が存在する場合には、それらを充足していることを要件とする。

【００８２】上記実施の形態では、一方向性関数としてハッシュ関数を例示したが、他の関数でもよい。上記実施の形態においては、クライアントとアクセスポイントの間の通信を例にこの発明を説明したが、この発明はこれに限定されず、２つの装置の間で暗号通信を行う場合に広く適用可能である。また、無線ＬＡＮを例に、この発明を説明したが、この発明は無線ＬＡＮに限定されず、その他の無線通信にも適用可能である。さらに、有線通信にも適用可能である。有線通信の場合には、無線ＬＡＮカード１２が、ＬＡＮカードに、無線ＩＦ２１１が有線ＩＦに変更される以外、実体的な変更はない。

【００８３】なお、この発明のシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体（フレキシブルディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行するサーバ１１１等を構成することができる。なお、上述の機能を、ＯＳが分担又はＯＳとアプリケーションの共同により実現する場合等には、ＯＳ以外の部分のみを媒体に格納してもよい。

【００８４】なお、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行させることにより、上述の処理を実行することができる。

【００８５】

【発明の効果】この発明によれば、信頼性の高い通信を行うことが可能となる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る通信システムの構成を示す図である。

【図２】図１に示すクライアント端末の構成を示す図である。

【図３】図１に示すアクセスポイントの構成を示す図である。

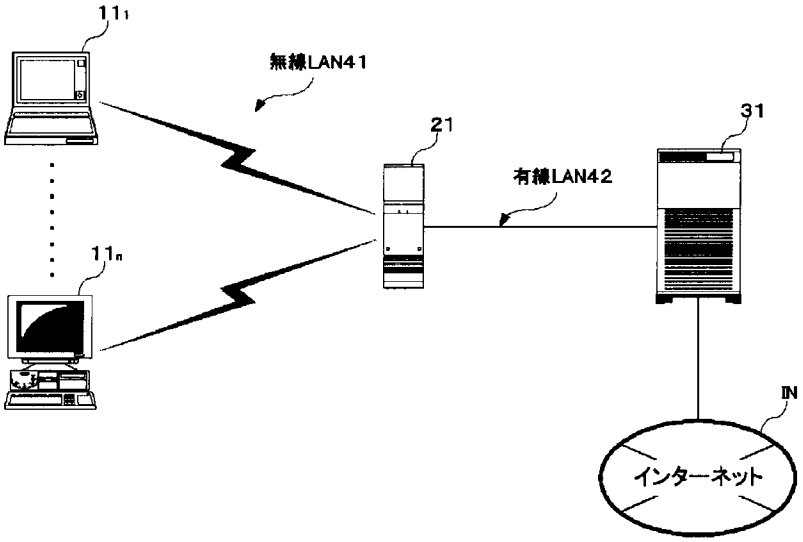
【図４】図３に示すデータベースに格納されるテーブルの例を示す図である。

【図５】第１の実施の形態において、クライアント端末とアクセスポイントとの間で送受信される情報とその手順を示す図である。

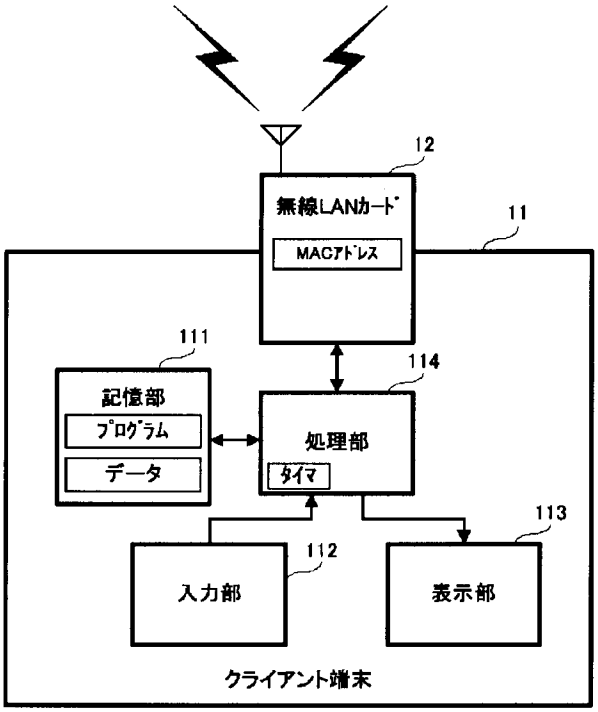
【符号の説明】

１１　クライアント端末
２１　アクセスポイント
４１　無線LAN
４２　有線LAN

【図１】



【図２】



【図４】

登録情報DB

(a)

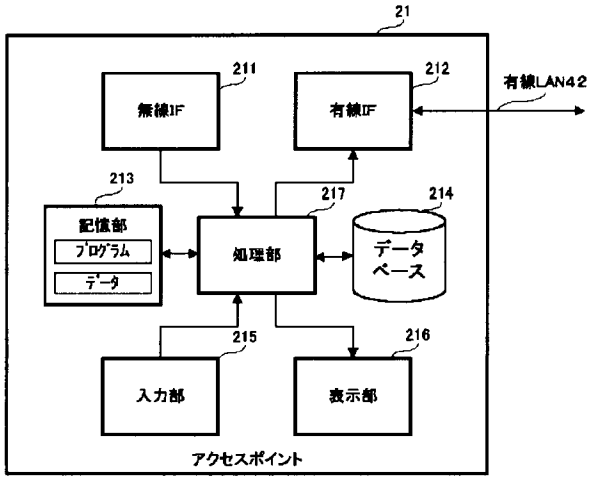
ID	PWD	生成日時T (yymmddmmss)
09801	3394416	0111310422
31287	2245525	0110180235
・	・	・

クライアント鍵DB

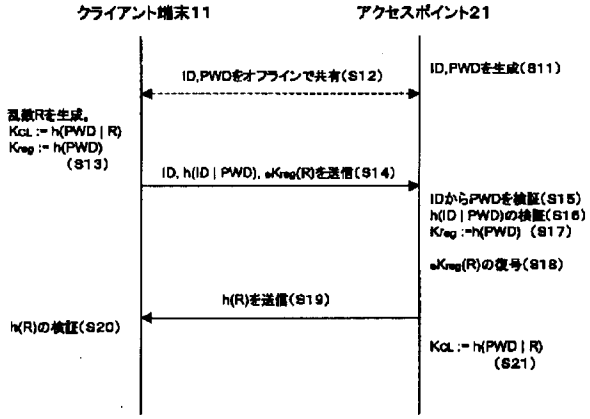
(b)

MACアドレス	KCL
00-20-af-f5-8a-30	0x09A1F54B2
00-40-c7-57-92-ef	0x12C4D6E81
・	・

【図３】


21
211
無線IF
212
有線IF
有線LAN42
213
記憶部
プログラム
データ
217
処理部
214
データベース
215
入力部
216
表示部
アクセスポイント

【図５】


クライアント端末11
アクセスポイント21
ID,PWDをオフラインで共有(S12)
ID,PWDを生成(S11)
乱数Rを生成。
KCL := h(PWD | R)
Kreg := h(PWD)
(S13)
ID, h(ID | PWD), eKreg(R)を送信(S14)
IDからPWDを検証(S15)
h(ID | PWD)の検証(S16)
Kreg :=h(PWD) (S17)
eKreg(R)の復号(S18)
h(R)を送信(S19)
h(R)の検証(S20)
KCL := h(PWD | R)
(S21)